# PATENT ABSTRACTS OF JAPAN

(11) Publication number : 11-250568
(43) Date of publication of application : 17.09.1999

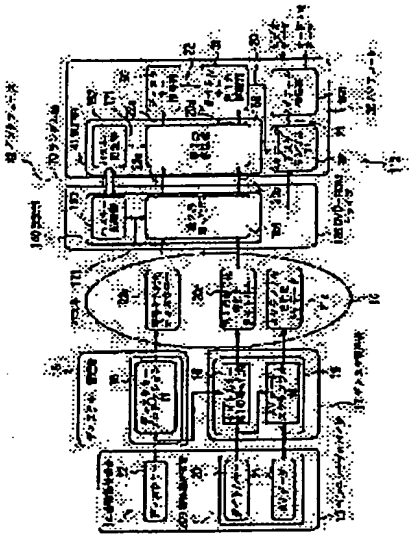
(51) Int. Cl. G11B 20/10

(21) Application number : 10-045846
(22) Date of filing : 26.02.1998

(71) Applicant : SONY CORP
(72) Inventor : MORI MASAHIRO
NAKAMURA TADASHI

## (54) READ-OUT DEVICE FOR RECORDING MEDIUM AND DATA PROCESSING DEVICE

(57) Abstract:
PROBLEM TO BE SOLVED: To provide a read-out device for an optical disk recording medium in which processing burden of a microcomputer can be lightened, in a DVD-ROM drive device.
SOLUTION: Key data 22a, 22b recorded in a DVD disk 10 and contents data 21a of which utilization is controlled by the key data are read out, read out key data 20a, 20b are ciphered by an authentication section 140, and the ciphered key data 20a, 20b and read out contents data 21a are transmitted to the outside through an interface 42. In the authentication section 140, data transfer accompanied by ciphering processing is controlled by a DMA section provided independently of the microcomputer performing servo control of rotation of the DVD disk and the like.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The key data recorded on the record medium and the contents data by which use is managed with the key data concerned are read, and said read key data are enciphered. The enciphered key data concerned with said read contents data In the record-medium read-out equipment transmitted outside through an interface The 1st control means which performs in generalization control including the control which reads said key data and said contents data from said record medium at least in the record-medium read-out equipment concerned, A storage means to memorize said read key data and said contents data, It is record-medium read-out equipment which controls said key data transfer between an encryption means to encipher said key data memorized by said storage means, and said storage means and said encryption means, and has the 2nd control means in which said 1st control means was prepared separately.

[Claim 2] Said 1st control means, said storage means, said encryption means, said 2nd control means, and said interface are record-medium read-out equipment according to claim 1 connected through the internal bus.

[Claim 3] Said encryption means is record-medium read-out equipment according to claim 1 which enciphers said key data based on the random data which oneself generated, and the random data inputted through said interface.

[Claim 4] Said 1st control means is record-medium read-out equipment according to claim 1 which directs initiation of encryption processing to said 2nd control means.

[Claim 5] Said 2nd control means is record-medium read-out equipment according to claim 1 which uses the Direct-Memory-Access method.

[Claim 6] Said record medium is record-medium read-out equipment according to claim 1 which is an optical disk record medium.

[Claim 7] Said contents data are record-medium read-out equipment according to claim 1 which is image data.

[Claim 8] Said contents data are record-medium read-out equipment according to claim 1 which is image data and sound data.

[Claim 9] In the data processor which is read from a record medium and transmits the enciphered key data and the contents data by which use is managed with the key data concerned to decoder equipment from record-medium read-out equipment through an interface The 1st control means which performs in generalization control in the record-medium read-out equipment concerned said whose record-medium read-out equipment includes the control which reads said key data and said contents data from said record medium at least, A storage means to memorize said read key data and said contents data, An encryption means to encipher said key data memorized by said storage means based on the 1st random data which oneself generated, and the 2nd random data inputted from said decoder equipment through said interface, Said key data transfer between said storage means and said encryption means is controlled, and said 1st control means has the 2nd control means established separately. Said decoder equipment Said 1st random data inputted from said record-medium read-out equipment through said interface, A decode means to decode said enciphered key data which were inputted through said interface based on said 2nd random data which oneself generated, The data processor which has the contents data-processing means which makes available the contents data inputted through said interface using said decoded key data.

[Claim 10] With said record-medium read-out equipment, said 1st control means, said storage means, said encryption means, said 2nd control means, and said interface are a data processor according to claim 9 connected through the internal bus.

[Claim 11] Said 2nd control means is a data processor according to claim 9 which uses the Direct-Memory-Access method.

[Claim 12] Said record medium is a data processor according to claim 9 which is an optical disk record medium.

[Claim 13] Said contents data are a data processor according to claim 9 which is image data.

[Claim 14] Said contents data are a data processor according to claim 9 which are image data and

sound data.
[Claim 15] Said 1st control means is a data processor according to claim 9 which directs initiation of encryption processing to said 2nd control means.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[The technical field to which invention belongs] This invention relates to the record-medium read-out equipment and the data processor which read the data recorded on record media, such as a DVD disk.

[0002]

[Description of the Prior Art] In recent years, a DVD (Digital Video Disc) player and LSI for DVD-ROM (Read Only Memory) equipments are developed actively. The disk key encoded with the predetermined algorithm and the title key enciphered (Encryption) are recorded on DVD from a viewpoint of protection of copyrights, and a DVD player, a computer, etc. can be used no longer for recorded AV data (contents data) if the disk key and the enciphered title key these-encoded are not decoded and decoded, respectively. Here, only when a disk key is recorded on one DVD disk of one sheet and this is decoded, use of other data recorded on the DVD disk is permitted. Moreover, a title key is prepared in each of two or more contents recorded on the DVD disk, and use is permitted only for AV data of the contents corresponding to the decoded title key.

[0003] Drawing 4 is drawing for explaining a process until it reproduces AV data recorded on the DVD disk 10 using the DVD prayer 11 and a computer (DVD-ROM drive equipment) 12 from record of the disk key to the DVD disk 10, and a title key. As shown in drawing 4 , the copyright person 200 who is one person of a content provider 13 supplies the AV data 21 set as the object of copyright, and the published title key 20 to the disk manufacturer 17. Moreover, the copyright manager 14 who is one person of a content provider 13 publishes the disk key 22, and supplies this to the disk key manager 15. The disk key manager 15 encodes the disk key 22 in the disk key protection section 16. This encoded disk key 22a is recorded on the DVD disk 10.

[0004] The disk manufacturer 17 scrambles the AV data 21 using the title key 20 in AV data scramble section 19 while performing encryption of the 1st of the title key 20 in the title key encryption section 18 (Scramble). Moreover, the disk manufacturer 17 manufactures the DVD disk 10 which recorded the title key as which the 1st was enciphered, scrambled AV data, and disk key 22a encoded from the disk key manager 15.

[0005] After the DVD disk 10 is shipped, it is set to a user's DVD player 11. The DVD player 11 is the disk key decode section 30 first in playback actuation. If encoded disk key 22a is decoded and the decode concerned is successful Next, if the title key corresponding to the contents which had directions from the user is decoded in the title key decode section 31 using the decoded disk key concerned and it succeeds in the decode concerned Next, corresponding AV data are descrambled in the descrambling section 32 using the title key concerned (Descramble), and it outputs to a display 33 as AV data S11.

[0006] Moreover, DVD-ROM drive 35 and the AV decoder 36 are formed in the computer 12. DVD-ROM drive 35 and the AV decoder 36 -- for example, ATAPI (AT Attachment Packet Interface) or SCSI (Small Computer System Interface) etc. -- it connects through the interface 42. The authentication section (Authentication) 40 is formed in DVD-ROM drive 35. In DVD-ROM drive 35, it is decided by specification to the key data transmitted through an interface 42 that encryption predetermined in the authentication section 40 is performed. Moreover, the authentication section 41, the disk key decode section 30, the title key decode section 31, and AV data descrambling section 32 are formed in the AV decoder 36.

[0007] Drawing 5 is the block diagram of DVD-ROM drive 35 shown in drawing 4 . As shown in drawing 5 , DVD-ROM drive 35 is carrying out the configuration which connected RF signal-processing section 51, RAM52, and a microcomputer 53 to the data bus 55. Moreover, the authentication section 40 is connected to the microcomputer 53. The data bus 55 is connected to the interface 42.

[0008] Actuation of DVD-ROM drive 35 at the time of outputting hereafter AV data read from the DVD disk to the AV decoder 36 through an interface 42 and the so-called bus encryption actuation are explained. Drawing 6 is a flow chart for explaining this actuation. First, a DVD disk rotates according to the servo control from a microcomputer 53, and scrambled AV data, the title key as

which the 1st was enciphered, and the encoded disk key are outputted to RF signal-processing section 51 from an optical pickup 50. In RF signal-processing section 51, these data are memorized by RAM52 through a data bus 55, after processing of waveform shaping etc. is performed (step S1). And before starting bus actuation, a bus key is generated using the random data which oneself generated in the authentication section 40, and the random data inputted through the authentication section 41 shown in drawing 4 to an interface 42 and a microcomputer 53. The random data generated in the authentication section 40 are outputted to the authentication section 41 through a microcomputer 53 and an interface 42. And in the AV decoder 36, the same bus key as what was generated in the authentication section 40 is generated using the random data which the authentication section 41 generated, and the random data inputted from the authentication section 40.

[0009] Next, the title key which was memorized by RAM52 and as which the 1st was enciphered is read to a microcomputer 53 through a data bus 55 before playback of a title (step S2). Next, the title key which was read to the microcomputer 53 and as which the 1st was enciphered is outputted to the authentication section 40 (step S3). And in the authentication section 40, the 2nd is further enciphered for the title key as which the 1st was enciphered based on the bus key generated as mentioned above (step S4). Next, the title key as which the 2nd was enciphered is read from the authentication section 40 to a microcomputer 53 (step S5). Next, the title key which was read to the microcomputer 53 and as which the 2nd was enciphered is returned to RAM52 through a data bus 55 (step S6).

[0010] And the title key by which the 2nd was enciphered as scrambled AV data which were memorized by RAM52 is outputted to the AV decoder 36 shown in drawing 4 through a data bus 55 and an interface 42 (step S7). Next, in the authentication section 41 of the AV decoder 36, the title key as which the 2nd was enciphered is decoded using the bus key mentioned above, and the title key as which the 1st was enciphered is generated. Next, at the time of disk insertion, using the disk key decoded in the disk key decode section 30, the title key as which the 1st was enciphered is decoded in the title key decode section 31, it descrambles scrambled AV data using the decoded title key concerned, and AV data are already generated. This AV data is outputted to a display 33, for example, after being elongated.

[0011]

[Problem(s) to be Solved by the Invention] however, in DVD-ROM drive 35 of the conventional computer 12 mentioned above Transmission of the title key as which the 1st from RAM52 to the authentication section 40 was enciphered as shown in drawing 6 (steps S2 and S3), Transmission (steps S5 and S6) of the title key as which the 2nd from the authentication section 40 to RAM52 was enciphered, and transmission of a disk key are performed through a microcomputer 53, and there is a problem that the processing burden of a microcomputer 53 is large. That is, although the processing in DVD-ROM drive 35 is controlled by the microcomputer 53 in generalization besides the servo control of DVD-ROM drive 35, while processing of steps S2, S3, S5, and S6 shown in drawing 6 etc. is performed, other control will be kept waiting and there is also a problem that a throughput declines.

[0012] This invention is made in view of the trouble of the conventional technique mentioned above, and it aims at offering the record-medium read-out equipment and the data processor which can mitigate the processing burden of a microcomputer in DVD-ROM drive equipment.

[0013]

[Means for Solving the Problem] Solve, and in order to attain the purpose which mentioned above the trouble of the conventional technique mentioned above, the record-medium read-out equipment of this invention The key data recorded on the record medium and the contents data by which use is managed with the key data concerned are read, and said read key data are enciphered. The enciphered key data concerned with said read contents data It is record-medium read-out equipment transmitted outside through an interface. The 1st control means which performs in generalization control including the control which reads said key data and said contents data from said record medium at least in the record-medium read-out equipment concerned, A storage means to memorize said read key data and said contents data, Controlling said key data transfer between

an encryption means to encipher said key data memorized by said storage means, and said storage means and said encryption means, said 1st control means has the 2nd control means established separately.

[0014] With the record-medium read-out equipment of this invention, the key data and contents data which were recorded on the record medium which rotated by the servo control by the 1st control means are read to the 1st storage means. Moreover, for example, initiation of encryption processing is directed to the 2nd control means from said 1st control means, the key data memorized by said storage means are outputted to an encryption means based on control of the 2nd control means, and the key data concerned are enciphered with said encryption means. Next, from said encryption means, said enciphered key data are transmitted to said storage means, and are memorized. Next, said enciphered key data which were memorized by said storage means are outputted outside through an interface. Here, contents data are image data, an application program, etc. with which a user is provided directly.

[0015] Moreover, the data processor of this invention is read from a record medium, and an interface is minded for the enciphered key data and the contents data by which use is managed with the key data concerned. It is the data processor transmitted to decoder equipment from record-medium read-out equipment. Said record-medium read-out equipment The 1st control means which performs in generalization control including the control which reads said key data and said contents data from said record medium at least in the record-medium read-out equipment concerned, A storage means to memorize said read key data and said contents data, An encryption means to encipher said key data memorized by said storage means based on the 1st random data which oneself generated, and the 2nd random data inputted from said decoder equipment through said interface, Controlling said key data transfer between said storage means and said encryption means, said 1st control means has the 2nd control means established separately. Said 1st random data which inputted said decoder equipment from said record-medium read-out equipment through said interface here, A decode means to decode said enciphered key data which were inputted through said interface based on said 2nd random data which oneself generated, It has the contents data-processing means which makes available the contents data inputted through said interface using said decoded key data.

[0016]

[Embodiment of the Invention] Hereafter, the DVD-ROM drive as record-medium read-out equipment concerning the operation gestalt of this invention is explained. Drawing 1 is a structure-of-a-system Fig. where DVD-ROM drive 135 of this operation gestalt is used. In drawing 1 , what attached the same sign as drawing 4 is the same as what was mentioned above. As shown in drawing 1 , the copyright person 200 who is one person of a content provider 13 supplies the AV data 21 set as the object of copyright, and the published title key 20 to the disk manufacturer 17. Moreover, the copyright manager 14 who is one person of a content provider 13 publishes the disk key 22, and supplies this to the disk key manager 15. The disk key manager 15 encodes the disk key 22 in the disk key protection section 16 while supplying the disk key 22 to the encryption section 18 of the disk manufacturer's 17 title key 1st. This encoded disk key 22a is recorded on the DVD disk 10.

[0017] Using the disk key 22, the 1st enciphers the title key 20 and, as for the title key encryption section 18, this title key 20a as which the 1st was enciphered is recorded on the DVD disk 10. Moreover, AV data scramble section 19 scrambles the AV data 21 in AV data scramble section 19 using the title key 20 (Scramble). This scrambled AV data 21a is recorded on the DVD disk 10. The DVD disk 10 with which encoded disk key 22a, title key 20a as which the 1st was enciphered, and scrambled AV data 21a were recorded by this is manufactured.

[0018] A computer 112 is the data processor of this invention, and has DVD-ROM drive 135 and the AV decoder 36. DVD-ROM drive 135 and the AV decoder 36 are connected through the interfaces 42, such as ATAPI or SCSI. The AV decoder 36 is the same as what is fundamentally shown in drawing 4 mentioned above.

[0019] DVD-ROM drive 135 DVD-ROM drive 135 has the authentication section 140. The authentication section 140 has the bus key processing section 150 and the 2nd encryption section

151. Before bus actuation initiation, based on the random data 172 which oneself generated, and the random data 170 inputted from the bus key processing section 152 through the interface 42, the bus key processing section 150 generates the bus key 171, and outputs this bus key 171 to the 2nd encryption section 151.

[0020] The 2nd encryption section 151 outputs disk key 22b as which the bus key 171 was used, the 2nd enciphered it, and this 2nd [ the ] enciphered encoded disk key 22a which was read from the DVD disk 10 at the time of insertion of the DVD disk 10 to the 2nd decode section 153 of the AV decoder 36 through an interface 42. Moreover, the 2nd encryption section 151 outputs title key 20b as which the bus key 171 was used, the 2nd enciphered it, and this 2nd [ the ] enciphered title key 20a as which the 1st read from the DVD disk 10 was enciphered at the time of playback of a title to the 2nd decode section 153 of the AV decoder 36 through an interface 42.

[0021] Moreover, DVD-ROM drive 135 outputs scrambled AV data 21a which was read from the DVD disk 10 to AV data descrambling section 32 of the AV decoder 36 through an interface 42.

[0022] The AV decoder 36AV decoder 36 has the authentication section 41, the disk key decode section 30, the decode section 31 of the title key 1st, AV data descrambling section 32, and AV data decompression section 160.

[0023] The authentication section 41 has the bus key processing section 152 and the 2nd decode section 153. In case the bus key processing section 152 inputs AV data 21a from DVD-ROM drive 135 through an interface 42, by the random value generator which is not illustrated, it generates the random data 170 and outputs this random data 170 to the bus key processing section 150 through an interface 42. Moreover, based on the random data 172 inputted from the bus key processing section 150 through the interface 42, and the random data 170, the bus key processing section 152 generates the bus key 171, and outputs this bus key 171 to the 2nd decode section 153. At this time, the bus key 171 which the bus key processing section 150 generates is the same as the bus key 171 which the bus key processing section 152 generates.

[0024] The 2nd decode section 153 decodes the disk key 22 as which the 2nd inputted through the interface 42 at the time of insertion of the DVD disk 10 was enciphered using the bus key 171, and generates encoded disk key 22a. The 2nd decode section 153 outputs disk key 22a to the disk key decode section 30. The 2nd decode section 153 decodes title key 20b as which the 2nd inputted through the interface 42 at the time of playback of a title was enciphered using the bus key 171, and generates title key 20a as which the 1st was enciphered. The 2nd decode section 153 outputs title key 20a to the decode section 31 of the title key 1st.

[0025] The disk key decode section 30 decodes encoded disk key 22a, generates the disk key 22, and outputs this to the decode section 31 of the title key 1st. Using the disk key 22, the decode section 31 of the title key 1st decodes title key 20a, generates the title key 20, and outputs this to AV data descrambling section 32. AV data descrambling section 32 descrambles scrambled AV data 21a which was inputted through the interface 42 using the title key 20, generates the AV data 21, and outputs this to AV data decompression section 160. AV data decompression section 160 elongates the AV data 21 compressed, generates AV data, and outputs this to a display.

[0026] Hereafter, DVD-ROM drive 135 is explained to a detail. Drawing 2 is the block diagram of DVD-ROM drive 135. As shown in drawing 2 , DVD-ROM drive 135 has the authentication section 140, an optical pickup 50, RF signal-processing section 51, RAM52, a microcomputer 53, and the DMA (Direct Memory Access) section 190. In drawing 2 , the component which attached the same sign as drawing 5 is the same as what was mentioned above. As shown in drawing 2 , DVD-ROM drive 135 is carrying out the configuration which connected the authentication section 140, RF signal-processing section 51, RAM52, and the DMA section 190 to the data bus 55. The microcomputer 53 is connected to the DMA section 190. Moreover, the data bus 55 is connected to the interface 42.

[0027] The DMA section 190 realizes access to RAM52 in which a microcomputer 53 does not participate, and, specifically, realizes data transfer between RAM52 and the authentication section 140. Actuation of DVD-ROM drive 135 at the time of outputting hereafter AV data read from the DVD disk 10 to the AV decoder 36 through an interface 42 is explained. Drawing 3 is a flow chart for explaining this actuation. First, a DVD disk rotates according to the servo control from a

microcomputer 53, and scrambled AV data 21a, title key 20a as which the 1st was enciphered, and encoded disk key 22a are outputted to RF signal-processing section 51 from an optical pickup 50. In RF signal-processing section 51, these data are memorized by RAM52 through a data bus 55, after processing of waveform shaping etc. is performed (step S11). And before starting bus actuation, a bus key is generated using the random data which oneself generated in the authentication section 140, and the random data inputted through the authentication section 41 shown in drawing 1 to the interface 42. The random data generated in the authentication section 140 are outputted to the authentication section 41 through an interface 42. And in the AV decoder 36, the same bus key as what was generated in the authentication section 140 is generated using the random data which the authentication section 41 generated, and the random data inputted from the authentication section 140.

[0028] Moreover, initiation of bus encryption actuation is directed in the DMA section 190 from a microcomputer 53 (step S12).

[0029] Next, title key 20a which was memorized by RAM52 and as which the 1st was enciphered is read to the authentication section 140 through a data bus 55 before playback of a title by control by the DMA section 190 (step S13). Next, in the authentication section 140, the 2nd is further enciphered for title key 20a as which the 1st was enciphered based on the bus key 171 (step S14). Title key 20b as which the 2nd was enciphered is generated by this.

[0030] Next, title key 20b as which the 2nd was enciphered is read from the authentication section 140 to RAM52 through a data bus 55 by control by DMA190 (step S15). That is, control of processing of steps S13-S15 is automatically performed by not the microcomputer 53 but the DMA section 190. Next, title key 20b which was memorized by RAM52 and as which scrambled AV data 21a and the 2nd were enciphered is outputted to the AV decoder 36 through a data bus 55 and an interface 42 (step S16).

[0031] And in the AV decoder 36, title key 20b as which the 2nd was enciphered in the 2nd encryption section 151 using said bus key 171 in the bus key processing section 152 is decoded, and title key 20a as which the 1st was enciphered is generated. This title key 20a as which the 1st was enciphered is outputted to the decode section 31 of the title key 1st.

[0032] In the decode section 31 of the title key 1st, title key 20a as which the 1st was enciphered using the title key already mentioned above and the disk key 22 decoded in the disk key decode section 30 through the same process at the time of disk insertion is decoded, and the decoded title key 20 concerned is outputted to AV data descrambling section 32. In AV data descrambling section 32, it descrambles scrambled AV data 21a using the title key 20, and the AV data 21 are generated. This AV data 21 is outputted to a display 33, for example, after being elongated.

[0033] As explained above, according to DVD-ROM drive 135, a transfer of RAM52, the authentication section 140, the title key of a between, and a disk key is realized not by control by the microcomputer 53 but by control by the DMA section 190. Therefore, after directing initiation of bus encryption actuation in the DMA section 190 in step S12 which shows a microcomputer 53 to drawing 3 , from the bus encryption processing concerned, it is opened wide, other processings can be performed and the processing burden of a microcomputer 53 is mitigated. Consequently, processing of a microcomputer 53 is accelerated.

[0034] This invention is not limited to the operation gestalt mentioned above. With the operation gestalt mentioned above, as a record medium, although the DVD disk was illustrated, especially if it has the specification as which encryption is required when transmitting record data through an interface, it will not be limited.

[0035]

[Effect of the Invention] As explained above, according to the record-medium read-out equipment and the data processor of this invention, the burden of processing of the 1st control means is mitigable.